(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09054547 A**

(43) Date of publication of application: **25.02.97**

(51) Int. Cl **G09C 1/00**
H04L 9/06

(21) Application number: **07206372**

(22) Date of filing: **14.08.95**

(71) Applicant: **NEC CORP**

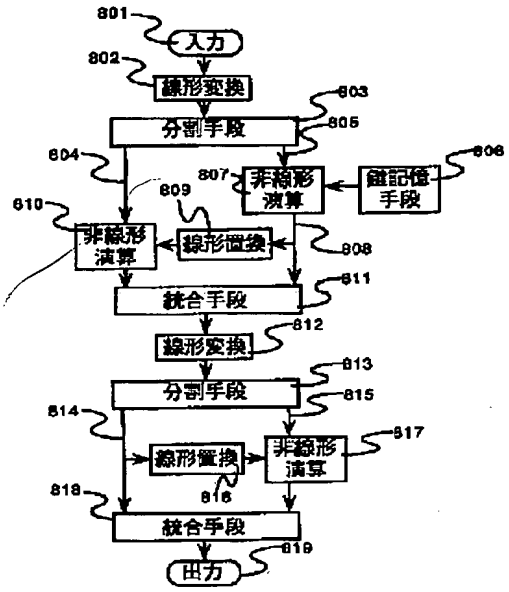
(72) Inventor: **MIYANO HIROSHI**

(54) **CIPHER DEVICE**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a cipher device having high safety for safeguarding data at the time of communication and storage of the data.

SOLUTION: Input 801 is divided to a bit string 805 and bit string 804 by a dividing means 803 after linear conversion 802. The bit string 805 is the input together with a key storage means 806 to nonlinear arithmetic operation 807. Linear substitution 809 is inputted with the output 808 of the nonlinear arithmetic operation 807 and nonlinear arithmetic operation 810 is inputted with the output of the linear substitution 809 and the bit string 804. The output 808 and the output of the nonlinear arithmetic operation 810 are integrated by an integrating means 811 and the output receives linear conversion 812 and is divided to a bit string 815 and a bit string 814 by a dividing means 813. The bit string 814 is subjected to nonlinear arithmetic operation 817 together with the output 815 after linear substitution 816 with a direct integrating means 818 and is inputted to the integrating means 818, by which the bit string is integrated to output 819.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－54547

(43)公開日　平成９年(1997)２月25日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０９Ｃ	1/00	６１０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６１０Ｃ
Ｈ０４Ｌ	9/06			Ｈ０４Ｌ	9/00	６１１Ｂ

審査請求　有　　請求項の数３　ＯＬ　（全 ９ 頁）

(21)出願番号　特願平7－206372

(22)出願日　平成７年(1995)８月14日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　宮野　浩
東京都港区芝五丁目７番１号　日本電気株式会社内

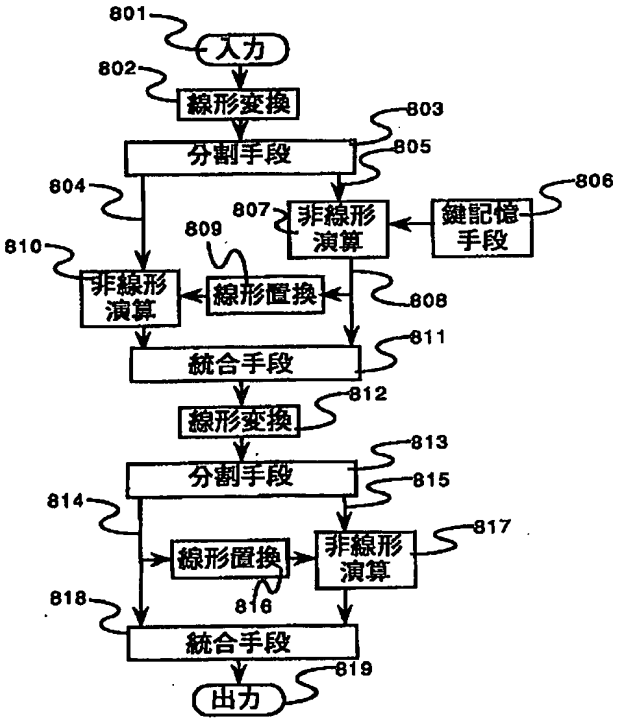
(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　暗号装置

(57)【要約】　（修正有）

【課題】　データの通信や蓄積の際にデータを秘匿するための安全性の高い暗号装置を提供する。

【解決手段】　入力８０１は線形変換８０２後、分割手段８０３でビット列８０５とビット列８０４に分割される。ビット列８０５は、鍵記憶手段８０６とともに非線形演算８０７の入力となる。線形置換８０９は非線形演算８０７の出力８０８を入力し、非線形演算８１０は線形置換８０９の出力とビット列８０４を入力する。出力８０８と非線形演算８１０の出力は統合手段８１１で統合され、出力は線形変換８１２を受け、分割手段８１３でビット列８１５とビット列８１４に分割される。ビット列８１４は直接統合手段８１８と、線形置換８１６の後、出力８１５と共に非線形演算８１７されて統合手段８１８へ入力して統合され、出力８１９となる。



1

【特許請求の範囲】

【請求項１】入力データを鍵に依存して暗号化する暗号装置であって、入力データを複数の同一データ長の部分データに分割する第１の分割手段と、複数個のデータ攪拌手段と、複数個の同一データ長の部分データを統合する第１の統合手段を有し、前記各々のデータ攪拌手段は、前記部分データの少なくとも１つを入力とし、該部分データと同一のデータ長のデータを出力とし、内部に有する鍵記憶手段内に記憶された鍵に依存したデータ変換処理を行うデータ変換手段を少なくとも１つ有し、該データ変換手段の出力を複数の部分データの１つに作用させることを特徴とする暗号装置において、

前記データ変換手段が、鍵を記憶する鍵記憶手段と、前記データ攪拌手段の入力に線形変換を施す第１の線形変換手段と、該第１の線形変換手段の出力をそれぞれ同一の長さの第１のビット列と第２のビット列に分割する第２の分割手段と、該第１のビット列に前記鍵記憶手段に記憶された鍵を作用させて非線形演算を行う第１の非線形演算手段と、該第１の非線形演算の出力に線形置換を施す第１の線形置換手段と、前記第２のビット列に該第１の線形置換手段の出力を作用させて非線形演算を行う第２の非線形演算手段と、前記第１の非線形演算手段の出力と該第２の非線形演算手段の出力とを連結してひとつのビット列とする第２の統合手段と、該第１の統合手段の出力に線形変換を施す第２の線形変換手段と、該第２の線形変換手段の出力をそれぞれ同一の長さの第３のビット列と第４のビット列に分割する第３の分割手段と、該第４のビット列に線形置換を施す第２の線形置換手段と、前記第３のビット列に該第２の線形置換手段の出力を作用させて非線形演算を行う第３の非線形演算手段と、該第３の非線形演算手段の出力と前記第４のビット列とを連結してひとつのビット列として出力する第３の統合手段とを備えることを特徴とする暗号装置。

【請求項２】請求項１に記載の暗号装置において、前記データ変換手段が、第３の統合手段の出力と前記鍵記憶手段に記憶された鍵とを入力として該鍵と同一のビット長のデータを生成し該生成されたデータを前記鍵記憶手段に記憶させる鍵更新手段を備えることを特徴とする暗号装置。

【請求項３】請求項１又は請求項２に記載の暗号装置において、

データ変換手段の有する線形変換手段の少なくとも１つが、該線形変換手段の入力を入力とする線形置換手段と、該線形置換手段の出力と前記線形変換手段の入力とを入力とする演算手段とを備えることを特徴とする暗号装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、データの通信や蓄積の際にデータを秘匿するための暗号装置に関する。

2

【０００２】

【従来の技術】ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）と呼ばれる暗号方式（特開昭５１－１０８７０１号公報「暗号装置」）に代表される共通鍵暗号の多くは、比較的簡単な変換操作を繰り返し行うことによって複雑な暗号化変換を実現することを特徴としている。図１は、多くの共通鍵暗号方式に採用されている暗号化手順の代表的な例を示したブロック図である。

【０００３】入力されたテキスト１０１は、分割手段１０２において第１のテキスト１０３と第２のテキスト１０４に分割される。この例においては、入力１０１が直ちに分割手段１０２の入力となっているが、入力に線形置換を施したり、あるいは暗号鍵に基づいて生成されたビット列とのビット毎の排他的論理和をとるなど、入力１０１に何らかの可逆な処理をほどこしたものを分割手段１０２の入力とするような構成をとるような暗号方式もある。第１のテキスト１０４および第２のテキスト１０４は攪拌手段１０５の入力となる。攪拌手段１０５による処理を繰り返された後、統合手段１０６は攪拌手段によって攪拌された第１の攪拌済みテキスト１０９と第２の攪拌済みテキスト１１０とを統合して出力１１１とする。前記攪拌手段１０５はデータ変換手段１０７を内蔵し、該変換手段１０７の出力と前記第２のテキストとのビット毎の排他的論理和をとった値で第２のテキストが置き換えられる。

【０００４】このような構成をとる暗号方式としては、ＤＥＳ以外には、ＦＥＡＬ（宮口庄司ら“Ｆａｓｔ　ｄａｔａ　ｅｎｃｒｙｐｔｉｏｎ　ａｌｇｏｒｉｔｈｍ　ＦＥＡＬ－８”，Ｒｅｖｉｅｗ　ｏｆ　ｅｌｅｃｔｒｉｃａｌ　ｃｏｍｍｕｎｉｃａｔｉｏｎｓ　ｌａｂｏｒａｔｏｒｉｅｓ，Ｖｏｌ．３６　Ｎｏ．４，１９８８）などが提案されている。

【０００５】これらの暗号方式は、データ変換手段１０７の内部構造によって特徴づけられる。

【０００６】図２はＤＥＳのデータ変換手段１０７の構成を示したものである。図２を用いてＤＥＳのデータ変換手段の構成を説明する。

【０００７】３２ビットからなるデータ変換手段の入力２０１は、拡大転置Ｅ２０２によって４８ビットに拡張される。この４８ビットと、鍵記憶手段２０２に記憶されている４８ビットの鍵との間でビット毎の排他的論理和２０４が計算される。非線形関数部２０５はS_1からS_8までの８つの非線形関数からなる。それぞれの非線形関数はいずれも入力ビット長が６ビット、出力ビット長が４ビットである。排他的論理和２０４の出力４８ビットは、先頭から順に６ビット毎、８つの部分に区切られ、それぞれ順にS_1，S_2，・・・，S_8の入力となる。８つの非線形変換の出力の合計３２ビットは、転置Ｐ２０６によって転置され、その結果が出力２０７とな

る。

【０００８】図３は拡大転置Ｅ２０２の機能を表した表である。拡大転置Ｅ２０２は入力長３２ビット、出力長４８ビットの関数である。この表は、たとえばこの表の先頭の「３２」という数字は拡大転置Ｅ２０２の出力の最初のビットは入力の３２番目と一致することを表しており、この表の２番目の「１」という数字は拡大転置Ｅ２０２の出力の２番目のビットは入力の１番目と一致することを表しているというように、拡大転置Ｅ２０２の出力の４８ビットと入力の３２ビットの関係を表している。

【０００９】図４は図３の非線形関数部２０５の８つの非線形関数S_1，S_2，・・・，S_8のうち、S_1の機能を表した表である。他の７つの非線形関数も、S_1と同様にあらかじめ定められた表によって機能が規定されているが、ここではS_1の機能を規定した表の説明をすることによって、非線形関数部の概要の説明とする。各々の非線形変換２０５は入力長６ビット、出力長４ビットの関数である。４つの行はそれぞれ、入力の先頭のビットと最後のビットの組がそれぞれ（０，０）、（０，１）、（１，０）、（１，１）である場合に対応している。１６個の列はそれぞれ、入力の第２ビットから第５ビットまでの４つのビットを４桁の二進数とみなしたときに、この二進数が表している数字が０，１，２，・・・である場合に対応している。表の各数字は、出力の４ビットを４桁の二進数とみなしたときの値を表している。たとえば、入力が（０００００）であるとすると、先頭のビットと最後のビットの組が（０，０）であるからこれは表の一番上の行に対応し、第２ビットから第５ビットまでの４つのビットの組は（０００）であり これを４桁の二進数と見ると０に対応するので該当する行の先頭の列が対応するから、その部分に書かれている数字「１４」に対応する４桁の二進数（１１１０）が入力（０００００）に対応する出力である。このように、入力に対応する出力が表によって定められているのがＤＥＳのデータ変換手段１０７の非線形関数S_1，S_2，・・・，S_8の特徴である。

＊【００１０】図５は転置Ｐ２０６の機能を表した図である。転置Ｐ２０６は入力長３２ビット、出力長３２ビットの関数である。表の見方は図３の拡大転置Ｅ２０２の機能を表した表と同様で、たとえばこの表の先頭の「１６」という数字は転置Ｐ２０６の出力の最初のビットは入力の１６番目と一致することを表しており、この表の２番目の「７」という数字は転置Ｐ２０６の出力の２番目のビットとは入力の７番目と一致することを表しているというように、転置Ｐ２０６の出力の３２ビットと入力の３２ビットの関係を表している。

【００１１】図６はＦＥＡＬのデータ変換手段１０７の構成を示したものである。図６を用いてＦＥＡＬのデータ変換手段の構成を説明する。

【００１２】３２ビットからなるデータ変換手段の入力６０１は、８ビットずつの４つの部分に分割される。これらのうちの２番目の８ビットと３番目の８ビットは、これら自身と鍵記憶手段６０２に記憶されている１６ビットの鍵とのビット毎の排他的論理和で置き換えられ、さらに１番目の８ビットは自身と新たに置き換えられた２番目の８ビットとのビット毎の排他的論理和で置き換えられ、４番目の８ビットは自身と新たに置き換えられた３番目の８ビットとのビット毎の排他的論理和で置き換えられる。さらに、２番目の８ビットは自身と３番目の８ビットを入力とする非線形関数$S_1$６０３の出力で置き換えられ、３番目の８ビットは自身と２番目の８ビットとを入力とする非線形関数$S_0$６０４の出力で置き換えられ、１番目の８ビットは自身と２番目の８ビットとを入力とする非線形関数$S_0$６０５の出力で置き換えられ、４番目の８ビットは自身と３番目の８ビットとを入力とする非線形関数$S_1$６０６の出力で置き換えられ、これらの４つの８ビットが統合されて３２ビットの出力６０７となる。

【００１３】図６の非線形関数S_0，S_1は、いずれも８ビットからなる２つの入力と１つの出力をそれぞれ８桁の二進数とみなすと、それぞれ以下の式で表すことのできる関数である。

＊【００１４】

$$S_0(x, y) = rot_2(x+1 \mod 256)$$

$$S_1(x, y) = rot_2(x+y+1 \mod 256)$$

ただし、上の式でrot_2は２ビット分のビットのローテーションを表す。

【００１５】また、これらの既存の暗号方式に対して改良を施すことによって安全性を高めようとする研究も行われている。たとえば小山謙二ら“Ｈｏｗ ｔｏ Ｓｔｒｅｎｇｔｈｅｎ ＤＥＳ－ｌｉｋｅ Ｃｒｙｐｔｏｓｙｓｔｍｓ ａｇａｉｎｓｔＤｉｆｆｅｒｅｎｔｉａｌ Ｃｒｙｐｔａｎａｌｙｓｉｓ”，ＩＥＩＣＥ Ｔｒａｎｓ．Ｖｏｌ．Ｅ７６－Ａ Ｎｏ．１ Ｊａｎ １９９３などがこうした研究の一例である。

【００１６】図７を用いて、前記小山らによって提案さ※れた方式を説明する。

【００１７】図７の攪拌手段７０１および攪拌手段７０２は、図１における攪拌手段１０５に対応する。この方式は、それぞれの攪拌手段７０１，７０２同士の間に、データの内容に応じて右半分と左半分を交換する機能を有する交換手段を挿入することを特徴としている。図７では、ふたつの攪拌手段しか描かれていないが、通常はそれぞれの攪拌手段の間が図７に示した構成をとる。

【００１８】攪拌手段７０１は、データ変換手段７０３と、該データ変換手段の出力とデータの右半分とのビット毎の排他的論理和をとる手段７０４からなることは、

図１の構成と同様である。データ変換手段７０３は、たとえば図２や図６で説明したような構成をとることができる。交換制御手段７０５はデータの左半分７０６とデータの右半分７０７とを参照し、たとえば‘０’であるビットが偶数個のときには左右を交換し奇数個の時には交換しないというようなあらかじめ定められた規則によってデータの左右を交換するかどうかを決定する。この決定に応じて、交換手段７０８はデータの左右を交換し、あるいは交換しない。交換する場合にはデータの左半分７０６は右半分７１０となり、右半分７０７は左半分７０９となる。交換しない場合にはデータの左半分７０６はそのまま左半分７０９となり、右半分７０７はそのまま右半分７１０となる。こうして交換手段７０８によって交換され、あるいは交換されないデータは次の段の攪拌手段７０２の入力となる。

【００１９】図７に示した方式の他にも、既存の暗号を改良することによって安全性を高める方式が提案されている。たとえば、鍵記憶装置（図２の２０２や図６の６０２）に記憶された鍵を、１ブロック（６４ビット）暗号化する毎に更新することによって安全性を高める方式（特開平０６－２６６２８４号公報（特願平０５－０５０２７６号）「暗号化装置」）などである。

【００２０】

【発明が解決しようとする課題】前記ＤＥＳなどの従来の暗号技術に対していくつかの解読法（暗号を破る手法）が提案されている。代表的なものに差分解読法（Ｅｌｉ Ｂｉｈａｍら“Ｄｉｆｆｅｒｅｎｔｉａｌ Ｃｒｙｐｔａｎａｌｙｓｉｓ ｏｆ ＤＥＳ－ｌｉｋｅＣｒｙｐｔｏｓｙｓｔｅｍｓ”，ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ＣＲＹＰＴＯ’９０）や線形解読法（松井充「ＤＥＳ暗号の線形解読法（Ｉ）」、１９９３年暗号と情報セキュリティシンポジウムＳＣＩＳ９３－３Ｃ）などがある。

【００２１】ＤＥＳは、図２に示したデータ変換手段の各々の出力ビットがいずれも入力の６ビットと鍵の６ビットからしか影響を受けていないことが線形解読法による攻撃が効果的であるひとつの理由であることが報告されている（宮野浩「線形解読法に対して有利なＦ関数の構成法」、１９９５年暗号と情報セキュリティシンポジウムＳＣＩＳ９５－Ａ４．３，１９９５．）。ＦＥＡＬの場合には、非線形関数６０３，６０４，６０５，６０６に加法を用いているため、出力ビットは多くの入力ビットから影響を受けるが、一部のビットから受ける影響は加算の際に連続して繰り上がりが起こった時のみに受ける影響であるためきわめて小さい影響となっている。そのため、ＦＥＡＬについても線形解読法に対してあまり安全性が高くなっていない。

【００２２】このように、線形解読法に対する安全性が高くない暗号方式に対して、図７を用いて説明したような方法などで安全性を高くした場合でも、データ変換手段１０７を改良することによってさらに安全性を高くすることは可能である。

【００２３】以上、説明したような理由によって、図１のような構成を持つ暗号方式において高い安全性を実現するようなデータ変換手段１０７を構成することが要請されている。

【００２４】

【課題を解決するための手段】本発明の暗号装置は、入力データを鍵に依存して暗号化する暗号装置であって、入力データを複数の同一データ長の部分データに分割する第１の分割手段と、複数個のデータ攪拌手段と、複数個の同一データ長の部分データを統合する第１の統合手段を有し、前記各々のデータ攪拌手段は、前記部分データの少なくとも１つとを入力とし、該部分データと同一のデータ長のデータを出力とし、内部に有する鍵記憶手段内に記憶された鍵に依存したデータ変換処理を行うデータ変換手段を少なくとも１つ有し、該データ変換手段の出力を複数の部分データの１つに作用させることを特徴とする暗号装置において、前記データ変換手段が、鍵を記憶する鍵記憶手段と、前記データ攪拌手段の入力に線形変換を施す第１の線形変換手段と、該第１の線形変換手段の出力をそれぞれ同一の長さの第１のビット列と第２のビット列に分割する第２の分割手段と、該第１のビット列に前記鍵記憶手段に記憶された鍵を作用させて非線形演算を行う第１の非線形演算手段と、該第１の非線形演算の出力に線形置換を施す第１の線形置換手段と、前記第２のビット列に該第１の線形置換手段の出力を作用させて非線形演算を行う第２の非線形演算手段と、前記第１の非線形演算手段の出力と該第２の非線形演算手段の出力とを連結してひとつのビット列とする第２の統合手段と、該第１の統合手段の出力に線形変換を施す第２の線形変換手段と、該第２の線形変換手段の出力をそれぞれ同一の長さの第３のビット列と第４のビット列に分割する第３の分割手段と、該第４のビット列に線形置換を施す第２の線形置換手段と、前記第３のビット列に該第２の線形置換手段の出力を作用させて非線形演算を行う第３の非線形演算手段と、該第３の非線形演算手段の出力と前記第４のビット列とを連結してひとつのビット列として出力する第３の統合手段とを備えることを特徴とする。

【００２５】また本発明の暗号装置は、前記データ変換手段が、第３の統合手段の出力と前記鍵記憶手段に記憶された鍵とを入力として該鍵と同一のビット長のデータを生成し該生成されたデータを前記鍵記憶手段に記憶させる鍵更新手段を備えることを特徴とする。

【００２６】また本発明の暗号装置は、データ変換手段の有する線形変換手段の少なくとも１つが、該線形変換手段の入力を入力とする線形置換手段と、該線形置換手段の出力と前記線形変換手段の入力とを入力とする演算手段とを備えることを特徴とする。

【００２７】
【実施例】前記のように、図１のような構成を持つ暗号方式において高い安全性を実現するようなデータ変換手段１０７を構成することは重要な問題である。そのようなデータ変換手段を実現するためには、非線形関数の非線形効果がなるべく効率良くデータ全体に広がっていくように構成することが効果的である。本発明は、データ変換手段がこのような効果を持つように、データ変換手段内部に線形変換手段を組み込んでいる。以下、実施例に従って本発明を詳細に説明する。
【００２８】図８は、本発明の第１の実施例におけるデータ変換手段１０７の構成を表した図である。まず、全体の構成について説明し、線形変換８０２，８１２、非線形演算８０７，８１０，８１７、線形置換８０９，８１６の機能については後で述べる。
【００２９】該データ変換手段の入力８０１は線形変換手段８０２による処理を受けた後、分割手段８０３において第１のビット列８０４と第２のビット列８０５とに分割される。第１のビット列８０５は、鍵記憶手段８０６とともに第１の非線形演算手段８０７の入力となる。第１の線形置換８０９は該非線形演算８０７の出力８０８を入力とし、第２の非線形演算８１０は該第１の線形置換８０９の出力と前記２のビット列８０４とを入力とする。前記第１の非線形演算８０７の出力８０８と前記第２の非線形演算８１０の出力とは統合手段８１１で統合され、該統合手段８１１の出力は線形変換手段８１２において線形変換を受け、該線形変換手段８１２の出力は分割手段８１３において第３のビット列８１４と第４のビット列２１５とに分割される。第２の線形置換８１６は該第４のビット列８１５を入力とし、第３の非線形演算８１７は該第２の線形置換８１６の出力と前記第３のビット列８１４とを入力とする。該第３の非線形演算８１７の出力と前記第４のビット列８１５とは統合手段８１８で統合され、８１８の出力が該データ変換手段１０７の出力８１９となる。
【００３０】線形変換８０２は、入力データをＸとしたときに、たとえばrot_{12}（Ｘ）とＸ自身とのビット毎の排他的論理和を出力する装置として構成することができる。ここでrot_{12}とは、既に説明したように、１２ビット分のビットのローテーションを表す。
【００３１】図１０は図８の線形変換８１２の一構成例を示した図である。この例では、線形置換手段の一例として巡回置換手段を、演算手段としてビット毎の排他的論理和を用いている。巡回置換手段５０２にて入力５０１を入力しrot_{12}の演算を行い、この演算結果と入力５０１のビット毎の排他的論理和５０３を出力としている。この構成例の特徴は、出力から入力が一意に定まらないため、解析されにくいという点である。
【００３２】線形変換８１２は、入力データをＸとしたときに、たとえばrot_{11}とrot_{22}（Ｘ）とＸ自身とのビット毎の排他的論理和を出力する装置として構成することができる。
【００３３】図１１は図８の線形変換８０２の一構成例を示した図である。この例では線形置換手段の一例として巡回置換手段を、演算手段としてビット毎の排他的論理和を用いている。ここで、巡回置換手段４０２，４０３にてそれぞれrot_{11}，rot_{22}の演算を行い、これらの演算結果と入力４０１のビット毎の排他的論理和４０４を出力としている。この構成例の特徴は、出力がちょうど３つの入力ビットの影響を受けるため、この線形変換手段をデータ変換手段内に組み込んだ場合、データ変換手段の各出力ビットに影響を与える入力ビットの数が大きくなることである。
【００３４】非線形演算８０７，８１０，８１７は、ふたつの入力をＸ，Ｙとして、たとえば
Ｘ　ｘｏｒ　Ｙ　ｘｏｒ　rot_1（Ｘ　ａｎｄ　Ｙ）
を出力する装置として構成することができる。ここで、ｘｏｒとはビット毎の排他的論理和を表し、ａｎｄとはビット毎の論理積を表す。
【００３５】線形置換８０９は、たとえば入力を７ビットローテーションする装置として構成することができる。
【００３６】該実施例において、データ変換手段の出力８１９の３２番目とデータ変換手段の入力８０１と鍵記憶手段８０６に記憶されている鍵との関係を式に表したのが次の式である。この式において、Y_{32}はデータ変換手段の出力８１９の３２番目のビット、X_iはデータ変換手段の入力８０１のｉ番目のビット、K_iは鍵記憶手段８０６に記憶されている鍵のｉ番目のビットをそれぞれ表し、＋は排他的論理和、＊は論理積を表すものとする。

$$Y_{32}=K_2+K_4+K_{13}+K_{16}+X_{10}+X_{19}+X_{20}+X_{21}+X_{28}+X_{29}+X_{32}+K_{15}*(X_9+X_{20}+X_{31})+K_3*(X_8+X_{19}+X_{29})+K_1*(X_6+X_{17}+X_{27})+K_{12}*(X_6+X_{17}+X_{28})+(K_1+X_6+X_{17}+X_{27}+K_{16}*(X_{10}+X_{21}+X_{32}))*(X_8+X_{18}+X_{29})+(K_1+K_{12}+X_8+X_{18}+X_{27}+X_{28}+X_{29}+X_{16}*(X_{10}+X_{21}+X_{32})+(X_{16}+X_{10}+X_{21}+X_{32}+X_{15}*(X_9+X_{20}+X_{31}))*(X_7+X_{17}+X_{26})+K_{11}*(X_5+X_{11}+X_{32}))*(K_3+K_{15}+X_8+X_9+X_{19}+X_{20}+X_{29}+X_{31}+K_{14}*(X_8+X_{19}+X_{30})+K_2*(X_7+X_{18}+X_{28}))$$

論理積は非線形な演算であり、出力ビットが非線形な演算による影響を多く受けることによって暗号方式の安全性が高まる。前記の式から、本発明のデータ変換手段の出力８１９のビットが多くの非線形な演算による影響を受けていることがわかる。このことは、線形変換手段８０２，８１８が、これらの線形変換手段の入力とこの入力に対して線形置換（この実施例においてはビットのローテーション）を施した結果とで演算（この実施例にお

いてはビット毎の排他的論理和）を施す構成であるため、非線形演算８０７，８１０，８１７による非線形な演算の効果が効率よく拡散していることによる。

【００３７】図９は本発明の第２の実施例におけるデータ変換手段１０７の構成を表した図である。本実施例においては、該データ変換手段１０７の出力を得るに至る手順は図８に示した例と全く同じである。図８との差異は、本実施例においては鍵更新手段９２０が統合手段９１８の出力と鍵記憶手段９０６に記憶されている鍵とを入力として該鍵と同一のビット長のビット列を出力し、該出力を鍵記憶手段９０６に記憶するというものである。鍵更新手段９２０は、たとえば非線形演算９０７と同じ構成にし、鍵記憶手段９０６に記憶されている鍵と統合手段９１８の出力の上位１６ビットとを入力とするように構成することができる。

【００３８】

【発明の効果】以上詳細に説明したように、本発明によれば、データの通信や蓄積の際にデータを秘匿するための安全性の高い暗号装置を得ることができる。

【図面の簡単な説明】

【図１】多くの共通鍵暗号方式において採用されている暗号化手順の構成図である。

【図２】ＤＥＳのデータ変換手段の構成図である。

【図３】ＤＥＳのデータ変換手段における拡大転置Ｅの機能を示した図である。

【図４】ＤＥＳのデータ変換手段における非線形変換のうちのひとつの機能を示した図である。

【図５】ＤＥＳのデータ変換手段における転置Ｐの機能を示した図である。

【図６】ＦＥＡＬのデータ変換手段の構成図である。

【図７】既存の暗号方式の安全性を高める従来方式の特徴的部分を示した図である。

【図８】本発明の第１の実施例におけるデータ変換手段の構成図である。

【図９】本発明の第２の実施例におけるデータ変換手段の構成図である。

【図１０】本発明の線形変換８１２の構成図である。

【図１１】本発明の線形変換８０２の構成図である。

【符号の説明】

１０１　暗号装置の入力
１０２　第１のデータ分割手段
１０３　第１のテキスト
１０４　第２のテキスト
１０５　データ攪拌手段
１０６　第１のデータ統合手段
１０７　データ変換手段
１０８　ビット毎の排他的論理和
１０９　第１の攪拌済みテキスト
１１０　第２の攪拌済みテキスト
１１１　暗号装置の出力

２０１　データ変換手段の入力
２０２　拡大転置Ｅ
２０３　鍵記憶手段
２０４　ビット毎の排他的論理和
２０５　非線形関数部
２０６　転置Ｐ
２０７　データ変換手段の出力
４０１　入力
４０２　巡回置換手段１
４０３　巡回置換手段２
４０４　演算手段
４０５　出力
５０１　入力
５０２　巡回置換手段
５０３　演算手段
５０４　出力
６０１　データ変換手段の入力
６０２　鍵記憶手段
６０３　非線形関数S_1
６０４　非線形関数S_0
６０５　非線形関数S_0
６０６　非線形関数S_1
６０７　データ変換手段の出力
７０１　データ攪拌手段
７０２　データ攪拌手段
７０３　データ攪拌手段
７０４　ビット毎の排他的論理和
７０５　交換制御手段
７０６　データの左半分
７０７　データの右半分
７０８　交換手段
７０９　データの左半分
７１０　データの右半分
８０１　データの変換手段の入力
８０２　第１の線形変換
８０３　第２のデータ分割手段
８０４　第２のビット列
８０５　第１のビット列
８０６　鍵記憶手段
８０７　第１の非線形演算
８０８　第１の非線形演算２０７の出力
８０９　第１の線形置換
８１０　第２の非線形演算
８１１　第２のデータ統合手段
８１２　第２の線形変換
８１３　第３のデータ分割手段
８１４　第４のビット列
８１５　第３のビット列
８１６　第２の線形置換
８１７　第３の非線形演算

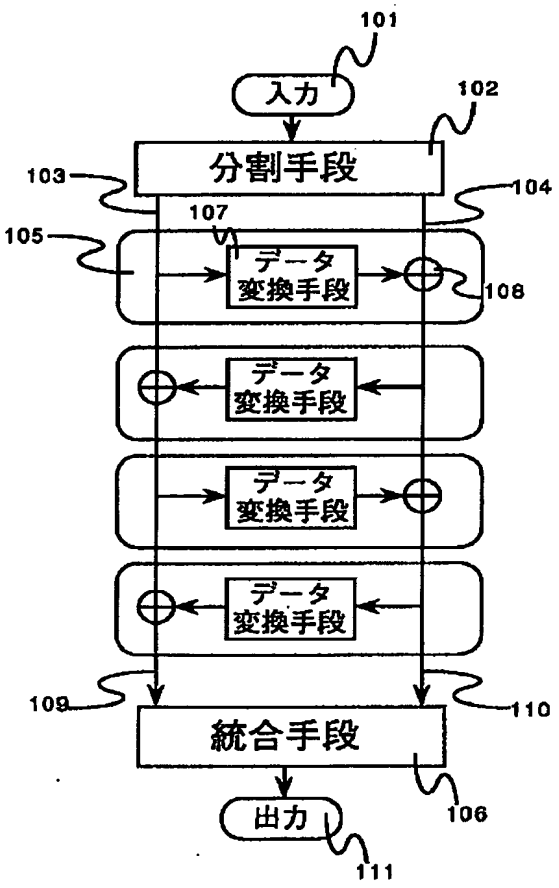
11

８１８　第３のデータ統合手段
８１９　データ変換手段の出力
９０１　データ変換手段の入力
９０２　線形変換
９０３　データ分割手段
９０４　ビット列
９０５　ビット列
９０６　鍵記憶手段
９０７　非線形演算
９０８　非線形演算３０７の出力
９０９　線形置換

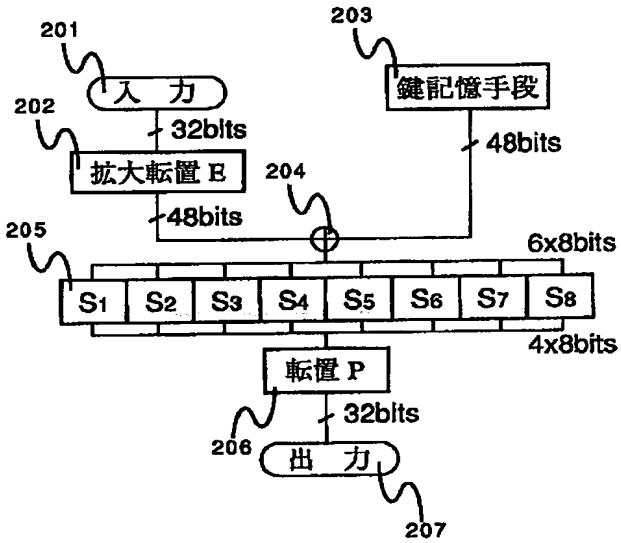
12

＊９１０　非線形演算
９１１　データ統合手段
９１２　線形変換
９１３　データ分割手段
９１４　ビット列
９１５　ビット列
９１６　線形置換
９１７　非線形演算
９１８　データ統合手段
９１９　データ変換手段の出力
＊　９２０　鍵更新手段

【図１】



【図２】



【図３】

拡大転置 E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

【図４】

S_1 の関数表

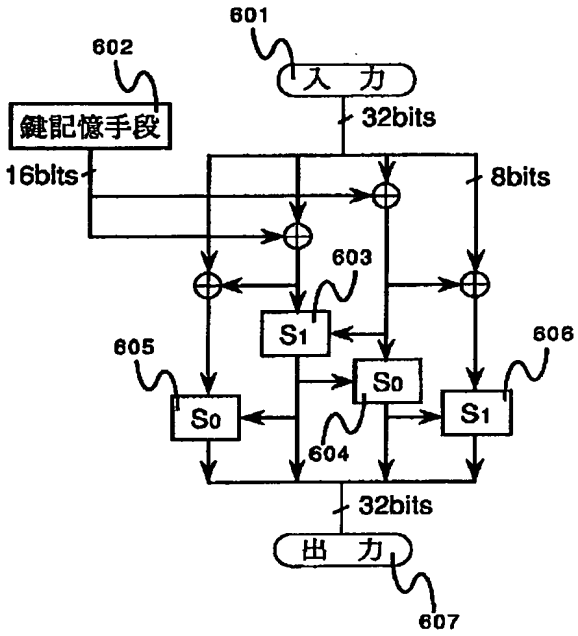
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

【図５】

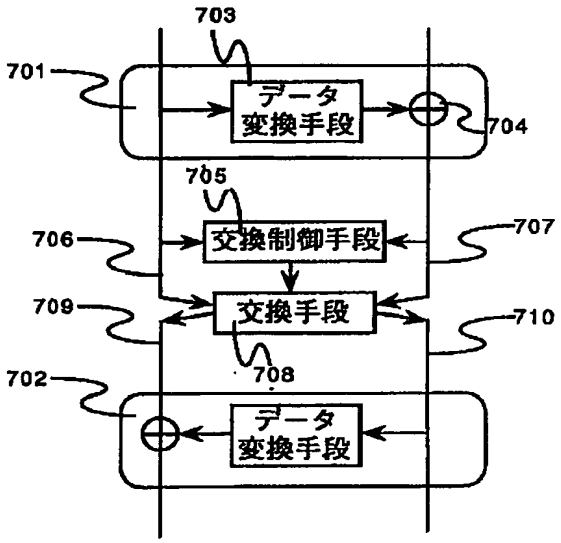
転置P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

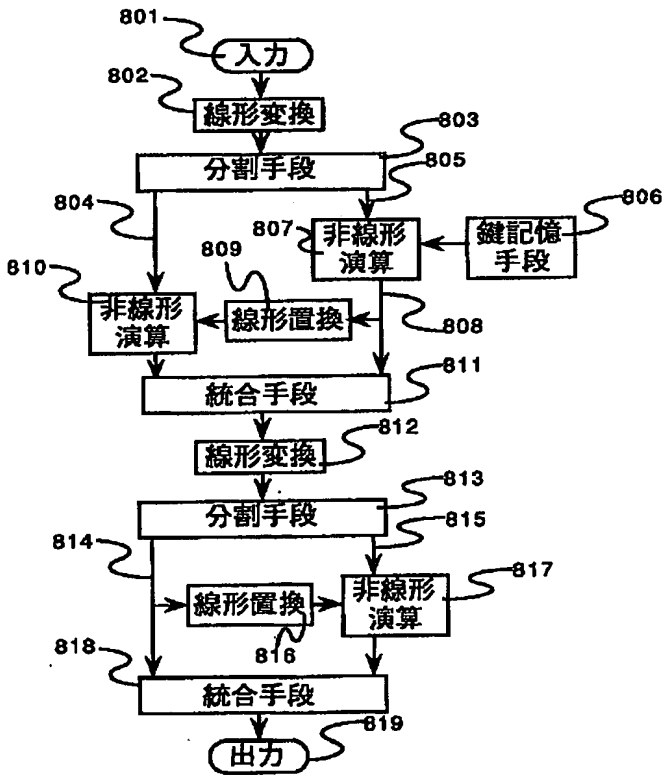
【図６】


601
602
入　力
鍵記憶手段
32bits
16bits
8bits
603
S1
605
606
S0
S0
S1
604
32bits
出　力
607

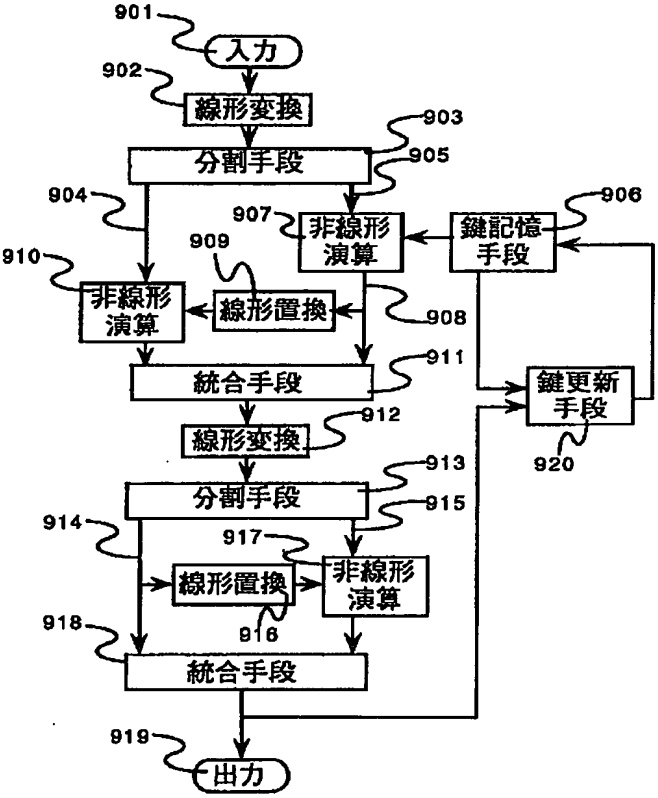
【図７】


703
701
データ
変換手段
704
705
交換制御手段
706
707
709
交換手段
710
708
702
データ
変換手段

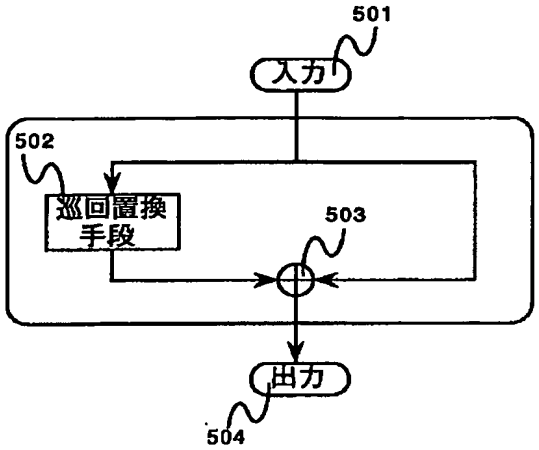
【図８】


801
入力
802
線形変換
803
分割手段
805
804
807
非線形
演算
鍵記憶
手段
806
809
810
非線形
演算
線形置換
808
統合手段
811
線形変換
812
813
分割手段
815
814
817
線形置換
非線形
演算
816
818
統合手段
出力
819

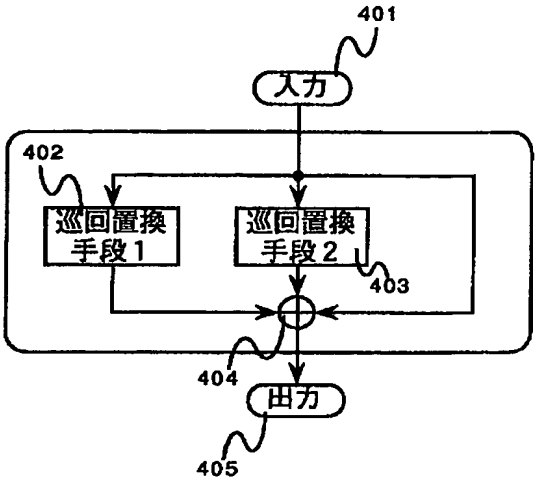
【図９】


901
入力
902
線形変換
903
分割手段
905
904
907
非線形
演算
鍵記憶
手段
906
909
910
非線形
演算
線形置換
908
統合手段
911
鍵更新
手段
912
線形変換
920
913
分割手段
915
914
917
線形置換
非線形
演算
916
918
統合手段
919
出力

【図１０】


501
入力
502
巡回置換
手段
503
出力
504

【図１１】


401
入力
402
巡回置換
手段１
巡回置換
手段２
403
404
出力
405